3 システムのセットアップ

本体を設置し、ケーブルを接続したあと、システムのセットアップをします。システムのセットアップは購入後、初めてセットアップする場合と再セットアップする場合に分けて説明しています。

初めてのセットアップ

購入後、初めてシステムをセットアップする時の手順について順を追って説明します。

初期導入設定用ディスクの作成

「初期導入設定用ディスク」は装置を導入するために最低限必要となる設定情報が保存されたセットアップ用のフロッピーディスクです。

「初期導入設定用ディスク」は、添付の初期導入設定用ディスクにある「初期導入設定ツール」を使って作成します。初期導入設定ツールは、Windows XP/2000、Windows NT、またはWindows Me/98/95で動作するコンピュータで動作します。

初期導入設定プログラムの実行と操作の流れ

Windowsマシンを起動して、次の手順に従って初期導入設定用ディスクを作成します。

1. Windowsマシンのフロッピーディスクドライブに添付の初期導入設定用ディスクをセットする。

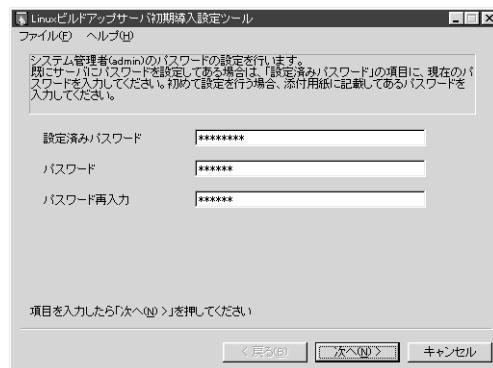
2. フロッピーディスクドライブ内の「初期導入設定ツール(startupConf.exe)」をエクスプローラなどから実行する。

   [Linuxビルドアップサーバ初期導入設定ツール]が起動します。プログラムは、ウィザード形式となっており、各ページで設定に必要事項を入力して進んでいきます。

   必須情報が入力されていない場合や入力情報に誤りがある場合は、次へ進むときに警告メッセージが表示されます。項目を正しく入力し直してください。入力事項については、この後の説明を参照してください。

   すべての項目の入力が完了すると、フロッピーディスクに設定情報を書き込んで終了します。

3. 初期導入設定用ディスクをフロッピーディスクドライブから取り出し、「システムのセットアップ」に進む。

   初期導入設定用ディスクは再セットアップの際にも使用します。大切に保管してください。

各入力項目の設定

[Linuxビルドアップサーバ初期導入設定ツール]で入力する項目について説明します。

パスワード設定

システムのセットアップ完了後、管理PCからWebブラウザを介して、システムにログインする際のパスワードを設定します。この画面にある項目はすべて入力する必要があります。
パスワードは推測されにくく覚えやすいものを用意してください。

パスワードは画面に表示されません。タイプミスをしないよう注意してください。

設定済みパスワード

初めて設定する場合は、同梱の別紙「rootパスワード」に記載されたパスワードを入力してください。以前に設定を行っている場合は、設定されているパスワードを入力してください。

パスワード

設定するパスワードを入力してください。ここで入力したパスワードは、管理者(admin)でログインする場合に必要となります。パスワードを忘れたり、不正に利用されたりしないように、パスワードの管理は厳重に行ってください。

なお、パスワードを変更したくない場合は、既存パスワードと同一のパスワードを新パスワードとして設定してください。

パスワード再入力

パスワードの確認用です。パスワードと同一のものを入力してください。

ネットワーク設定　～LANポート1(標準LAN)用～

LANポート1(標準LAN)のネットワーク設定をします。[セカンダリネームサーバ]以外は必ず入力してください。

ホスト名(FQDN)

ホスト名を入力してください。入力の際には、FQDNの形式 (マシン名.ドメイン名)の形式で入力してください。また、英字はすべて小文字で指定してください。大文字は使用できません。

IPアドレス

1枚目のNIC(LANポート1(標準LAN))に割り振るIPアドレスを指定してください。

サブネットマスク

1枚目のNIC(LANポート1(標準LAN))に割り振るサブネットマスクを指定します。

ディフォルトゲートウェイ

ディフォルトゲートウェイのIPアドレスを指定します。

プライマリネームサーバ

プライマリネームサーバのIPアドレスを指定します。

セカンダリネームサーバ

セカンダリネームサーバが存在する場合は、そのIPアドレスを指定します。

ネットワーク設定　～LANポート2(拡張LAN)用～

LANポート2(拡張LAN)のネットワーク設定をします。使用しない場合は、設定する必要はありません。

IPアドレス

2枚目のNIC(LANポート2(拡張LAN))に割り振るIPアドレスを指定してください。

サブネットマスク

2枚目のNIC(LANポート2(拡張LAN))に割り振るサブネットマスクを指定します。

初期導入設定プログラムでは増設ボードにより拡張したLANの設定を行うことはできません。Management Consoleのネットワーク設定にあるインタフェースで設定を行ってください。

システム構成条件の設定

Management Consoleの動作モードを設定します。
VirusCheckServerは[スタンドアロン構成]で動作します。

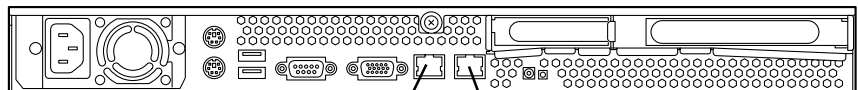
システムのセットアップ

初期導入設定ツールで作成した「初期導入設定用ディスク」を使用して、短時間でセットアップできます。

セットアップの手順

以下手順でセットアップをします。

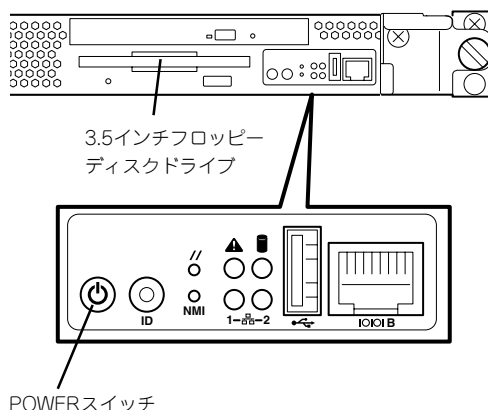
正しくセットアップできないときは、次ページ、および7章を参照してください。

1. 本体背面のLANポート1とLANポート2(使用する場合)にネットワークケーブルが接続されていることを確認する。

2. 前述の「初期導入設定用ディスクの作成」で作成した初期導入設定用ディスクを3.5インチフロッピーディスクドライブにセットする。

3. POWERスイッチを押す。

   POWERランプが点灯します。

   しばらくすると、初期導入設定用ディスクから設定情報を読み取り、自動的にセットアップを進めます。2〜3分ほどでセットアップが完了します。

   次項および4章を参照してシステムの状態確認や設定変更を行ってください。

重要

セットアップの完了が確認できたらセットした初期導入設定用ディスクをフロッピーディスクドライブから取り出して大切に保管してください。再セットアップの時に再利用することができます。

セットアップに失敗した場合

システムのセットアップに失敗した場合は、ビープ音を鳴らすことでユーザーに異常を知らせます(自動的に電源がOFF(POWERランプ消灯)になります)。正常にセットアップが完了しなかった場合は、初期導入設定用ディスクに書き出されるログファイル「logging.txt」の内容をコンピュータの「メモ帳」などのツールを使って確認し、再度初期導入設定ツールを使用して初期導入設定用ディスクを作成し直してください。

<主なログの出力例>

■「Info: completed.」

→ 正常にセットアップが完了した場合に表示されます。

■「Info: quitting with no change.」

→ 初期導入設定ツールを使って再度作成せずに、一度セットアップに使用した初期導入設定用ディスクを再使用した場合に表示されます(設定は反映されません)。

■「Cannot get authentication: root」

→ 初期導入設定用ディスク中のパスワードの指定に誤りがある場合に表示されます。

■「Error: invalid file: /mnt/floppy/linux.aut」

→ 初期導入設定用ディスク中のパスワード情報を格納したファイル(linux.aut)が正しく作成されなかった場合に表示されます。

■「Error: cannot open: /mnt/floppy/linux.aut」

→ 初期導入設定用ディスク中のパスワード情報を格納したファイル(linux.aut)が正しく作成されなかった場合に表示されます。

セットアップや運用時のトラブルについての対処を7章で詳しく説明しています。

セットアップの確認

本製品でウイルス検索、フィルタリング、ブロックなどの機能や、アップデート機能を利用する為にはアクティベーションの実施が必要です。
アクティベーションの実施は、InterScanコンソールより[管理]→[製品ライセンス情報]を選択しアクティベーションコードを入力して[アクティベート]を実行します。
本製品の出荷状態では、アクティベーション以外にも管理者の通知先設定など、お客様環境に合わせた詳細設定が必要です。
セットアップ実施後は、アクティベーションの実施を含め、パターンファイルのアップデートの実施など少なくとも1回はInterScanコンソールを開き、InterScan VirusWallの設定内容を確認するようにしてください。

重要 **InterScan VirusWallの詳細な設定は基本ライセンスに添付の「InterScan VirusWall for Small and Medium Businesses クイックスタートガイド」を参照してください。**

1. InterScanコンソールを開く。

   InterScanコンソールを開くには次の2つの方法があります。

   - Management Consoleからサービスのアイコンを選択し、[ウイルスチェック]をクリックする。
   - Webブラウザを起動し、InterScanマシンのIPアドレス：ポート番号(HTTP=1812、HTTPS=8443)のURLを入力する。

     IPアドレスの部分は、 InterScanマシンのドメイン名、 IPアドレスのいずれでもかまいません。次にHTTPの例を示します。

     http://ドメイン名:1812
     http://isvw.widget.com:1812
     http://123.12.123.123:1812

     HTTPSでログインする場合の例を示します。

     https://ドメイン名:8443
     https://isvw.widget.com:8443
     https://123.12.123.123:8443

2. InterScanコンソールにログインするためのパスワードを入力する。

   InterScanコンソールにはパスワードが設定されています。出荷時のパスワードは「password」です。

   重要

   管理者以外からの設定変更を防止するため、セットアップ完了後に新たなパスワードにパスワード変更を行ってください。

   パスワードはInterScanコンソールにログインするために必要ですので確実に保管してください。

ウイルスパターンファイル

ウイルスを検出するために、InterScan VirusWallでは、一般にウイルスパターンファイルと呼ばれる、ウイルスシグネチャの大規模なデータベースを利用しています。新しいウイルスが発生、検出された場合、トレンドマイクロ社ではそのシグネチャを収集して、ウイルスパターンファイルに情報を追加して新たなパターンファイルとして提供します。
ウイルスパターンファイルの命名規則は次のとおりです。

lpt$vpn.###

###は、パターンファイル番号(たとえば505)を表します。同じディレクトリに複数のファイルが存在する場合、最も新しいファイルのみが使用されます。
トレンドマイクロ社では、ほぼ毎週新しいウイルスパターンファイルを提供していますので、少なくとも1週間ごとにパターンファイルをアップデートするようにしてください。登録ユーザは、アップデートファイルを入手することができます。アップデートファイルは、インターネット経由で自動的にダウンロードすることができます。

重要

古いパターンファイルを手動で削除する必要はなく、また新しいファイルを使用するために、特別なインストール手順を実行する必要はありません。後述の[手動アップデート]をクリックするだけで、システムが自動的に新しいパターンファイルを設定します。
InterScan VirusWallのアップデートでは次のファイルを自動的に最新版にアップデートします。

- **ウイルスパターンファイル**
- **検索エンジン**
- **スパムメール対策ルール**
- **スパムメール対策エンジン**

ウイルスパターンファイルを手動でアップデートする

ウイルスパターンファイルを手動でアップデートするには、InterScanコンソールを開き、[アップデート]→[手動アップデート]をクリックしてください。
アップデート実施時、本製品上のパターンファイルよりも新しいパターンファイルがトレンドマイクロ社より提供されている場合にのみ、アップデートが実行されます。

重要

ウイルスパターンファイルをアップデートするためにはアクティベーションの実施が必要です。本製品のセットアップ後、速やかにアクティベーションを実施してください。
アクティベーションの実施は、InterScanコンソールを開き、[管理]→[製品ライセンス情報]を選択し、アクティベーションコードを入力して[アクティベート]をクリックして実施してください。

ウイルスパターンファイルの自動アップデートを設定する

自動アップデートを設定するには、次の手順に従ってください。

1. InterScanコンソールを開き、[アップデート]をクリックする。

2. [予約アップデート]をクリックする。

   自動アップデートのためのオプションを設定する[予約アップデート]画面が表示されます。

3. **<ウイルスパターンファイルの自動アップデートを無効にする場合>**

   [予約アップデートを有効にする]のチェックをはずす。

   <ウイルスパターンファイルの自動アップデートを実行する場合>

   実行周期を設定する。
   また、必要に応じて、実行する時刻を[開始時刻]に設定してください。

HTTPプロキシサーバの使用

InterScan VirusWallでは、インターネット上のトレンドマイクロ社のサイトから、新しいウイルスパターンファイルを取得します。InterScan VirusWallとインターネットの間にHTTPプロキシサーバが設定されている環境で、このサイトにアクセスする場合には、HTTPプロキシサーバを指定して、プロキシサーバにログオンするための情報を指定する必要があります。

プロキシサーバを指定するには、次の手順に従ってください。

1. InterScanコンソールを開き、[アップデート]をクリックする。

2. [プロキシ設定]をクリックする。

   [プロキシサーバ設定]画面が表示されます。

3. InterScanとインターネットの間にプロキシサーバが存在する場合は、[HTTPプロキシを使用する]もしくは[Socks 4プロトコルを使用する]を選択(チェック)する。

   プロキシサーバが存在しない場合は、初期設定のまま上記選択のチェックをはずした状態にしておく。

   a. [サーバ:]に、プロキシサーバのドメイン名(またはIP アドレス)を入力します(例: proxy.company.com)。

   b. [ポート:]にプロキシサーバが使用するポート番号を入力します(例: 80または8080)。

4. プロキシサーバにログインする際にユーザ名、パスワードが必要な場合は、InterScanが使用するユーザ名とパスワードを、それぞれ[ユーザ名:]、[パスワード:]に入力する。

5. [保存]をクリックする。

InterScan VirusWallのユーザー登録

ユーザー登録は非常に大切な作業であり、InterScan VirusWallのユーザー登録を行うと、InterScan VirusWallを使用するためのアクティベーションコードが提供されると共に、次のサービスを受けることができます。
ユーザー登録はインターネット経由での登録となります。

- 1年間のウイルスパターンファイル等のアップデート
- 1年間のサポートサービス
- 製品の更新情報や新製品案内のご提供

ユーザー登録の方法は、基本ライセンスおよび本製品に添付されております使用許諾契約書に同梱されております冊子“トレンドマイクロ製品をお使いいただくために”に記載しておりますので、ご参照の上ユーザ登録の実施およびアクティベーションコードの取得を行ってください。
ユーザ登録の際に必要となりますレジストレーションキーは、基本ライセンスおよび本製品に添付されております使用許諾契約書に記載されております。

重要

本製品でウイルス検索、フィルタリング、ブロックなどの機能や、アップデート機能を利用する為にはアクティベーションの実施が必要です。
本製品のセットアップに先立ち、ユーザー登録およびアクティベーションコードの取得を実施してください。
ユーザ登録時に発行されるアクティベーションコードは非常に重要な情報です。確実に保管してください。

E-MAIL(SMTP)の設定

InterScan VirusWallのE-Mail(SMTP)検索は、現在お使いのSMTPサーバ(オリジナルSMTPサーバ)の前段に設置することでご利用いただくことができます。
設定詳細については、基本ライセンスに添付の「InterScan VirusWall for Small and Mediuam Businessesクイックスタートガイド」の第6章を参照してください。

重要

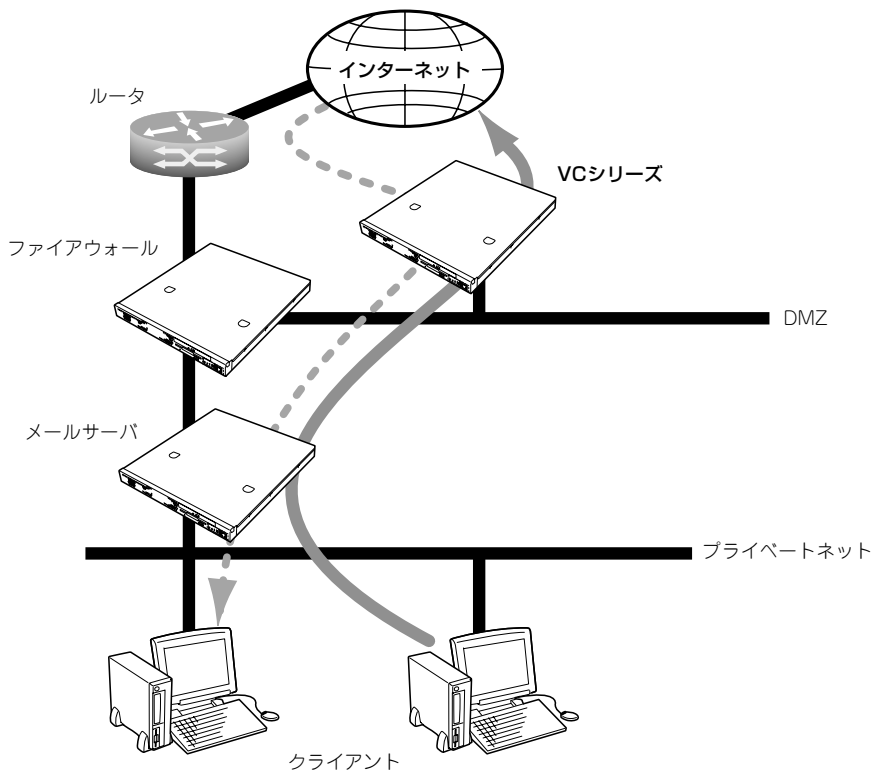
E-Mail検索では、受信メールを検索後にオリジナルSMTPサーバに配送する設定等が必要です。

[e-mail(SMTP)]→[設定]のサーバタブ画面、[SMTPサーバアドレスとポート]にInterScan VirusWallが受信するIPアドレス、ポート番号を設定します。
受信メールを配送するオリジナルSMTPサーバのIPアドレス、ポート番号を[受信メール配信：]の[次のSMTPサーバに配信する]に設定します。
送信メールの配信にもオリジナルSMTPサーバを使用する場合は、オリジナルSMTPサーバのIPアドレス、ポート番号を[送信メールの配信：]の[次のSMTPサーバに配信する]を選択して設定します。
DNS名前解決による送信メールの配信を使用する場合には、[送信メールの配信：]の[DNS名前解決を使用する]を選択します。
受信メール、送信メールの判断は、[e-mail(SMTP)]→[設定]の受信メールタブ画面の[SMTP受信メール]に指定されたドメイン宛のメールが受信メールと判断されます。
その他、SMTPセキュリティ強度の向上のため、その他の接続制限やリレー管理などの設定を行うことを強くお勧めします

InterScan VirusWallの動作

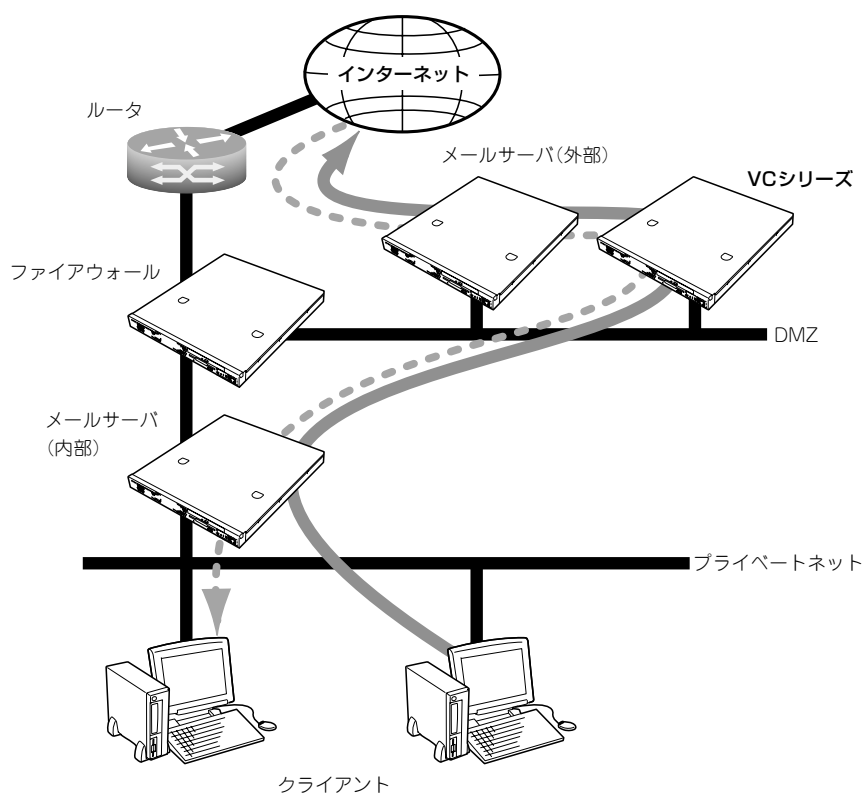
E-Mail VirusWallは、ポート番号25でSMTPトラフィックを受信後、対象となるトラフィックのウイルスを検索し、指定されたポート(ここでは25)を使用して、[Original SMTP server location]で指定された SMTPサーバにルーティングします。

VirusWallの導入例(E-Mail検索)

● **メールサーバが内部にある場合**

設定方法

1. DNSのMXレコードをVC300bへ変更する。
2. メールサーバが外部へのメールをVC300bに配送するように変更する。
3. VC300bが内部へのメールはメールサーバへ、外部へのメールはインターネットへ配送するように設定する。

   〔e-mail(SMTP)〕、〔設定〕の受信メールタブ画面のSMTP受信メール：の受信メールドメイン：に内部メールとして扱う宛先のドメインを全て指定します。
   〔e-mail(SMTP)〕、〔設定〕のサーバタブ画面の受信メール配信の"次のSMTPサーバに配送する"にメールサーバのIPアドレスとポート番号を指定します。
   送信メールの配信：に"DNS名前解決を使用する(MXレコード)"を選択します。

● メールサーバが外部と内部にある場合

設定方法

1. 外部メールサーバが内部へのメールをVC300bに配送するように変更する。

2. 内部メールサーバが外部へのメールをVC300bに配送するように変更する。

3. VC300bが外部メールサーバからのメールは内部メールサーバへ、内部メールサーバからのメールは外部メールサーバへ配送するように設定する。

   [e-mail(SMTP)]、[設定]の受信メールタブ画面のSMTP受信メール：の受信メールドメイン：に内部メールとして扱う宛先のドメインを全て指定します。
   [e-mail(SMTP)]、[設定]のサーバタブ画面の受信メール配信の"次のSMTPサーバに配送する"にメールサーバのIPアドレスとポート番号を指定します。
   [e-mail(SMTP)]、[設定]のサーバタブ画面の送信メールの配信：に"次のSMTPサーバに配送する"を選択し、外部メールサーバのIPアドレスとポート番号を指定します。

Web(HTTP)の設定

InterScan VirusWallのWeb(HTTP)検索は、お使いのシステムの設定に従って独自のProxyサーバとして設定することも、既存のHTTPプロキシサーバと併用することもできます。システムの設定に応じて、InterScanコンソールの[HTTP設定]ページで、[スタンドアロンモード]または、[プロキシサーバを使用する]のどちらかを選択します。

InterScan VirusWallのWeb(HTTP)検索でFTPトラフィックを検索する場合は、クライアント側のWebブラウザ設定で、InterScan VirusWallのWeb(HTTP)をFTPプロキシとして使用するように指定する必要があります。

HTTP設定：

InterScan VirusWallの管理コンソールで、[Web(HTTP)]→[設定]を選択し、[HTTP設定：]で、[スタンドアロンモード]、または[プロキシサーバを使用する]を選択し[プロキシサーバ：]と[ポート：]に既存のプロキシサーバのIPアドレスとポート番号を指定する。

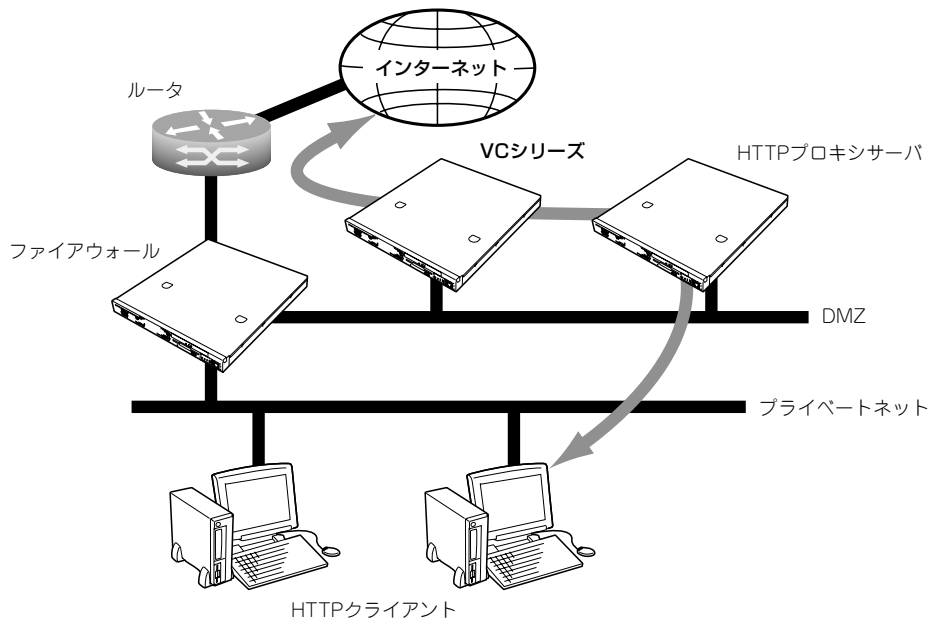
- **スタンドアロンモード**

  ネットワーク上に既存のHTTPプロキシサーバがなく、InterScan VirusWallのWeb(HTTP)をシステム全体のHTTPプロキシサーバとして使用する場合、またはInterScan VirusWallのWeb(HTTP)を論理上インターネットとプロキシサーバの間に配置する場合には、このオプションを選択します。

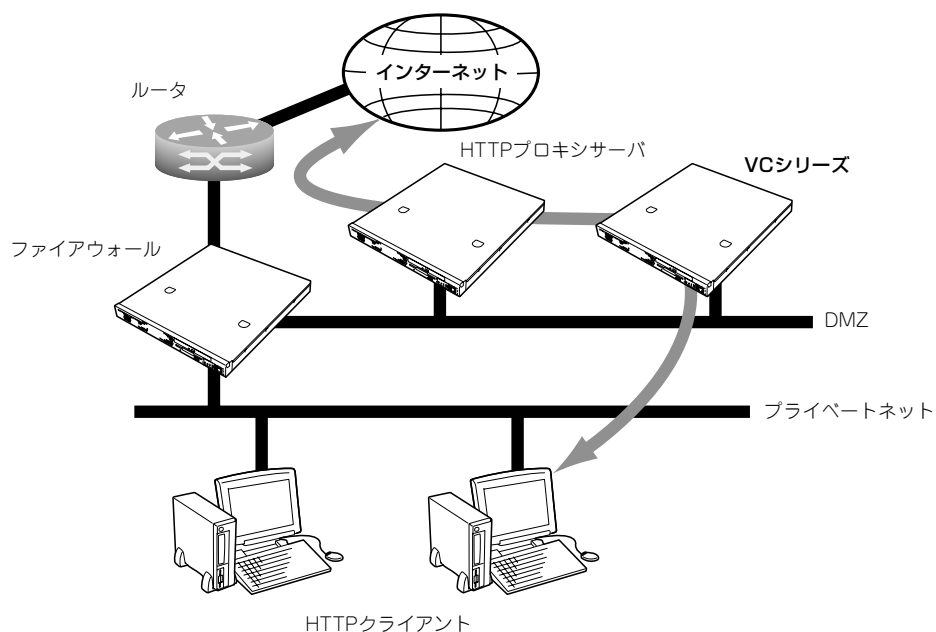
- **プロキシサーバを使用する**

  ネットワーク上に既存のHTTPプロキシサーバがある場合には、このオプションを選択し、IPアドレスとポート番号を入力します。InterScan VirusWallのWeb(HTTP)では、インターネットからInterScan VirusWallのWeb(HTTP)を経由する、ここで指定されたマシンへのHTTPトラフィックについてウイルス検索を行います

InterScan VirusWallの導入例（Web検索）

● HTTPプロキシサーバの上位にVC300bを設置する場合

設定方法

1. HTTPプロキシサーバの上位プロキシサーバとしてVC300bを設定する。
2. VC300bが直接インターネットを参照するプロキシサーバとして動作するように設定する。
   [Web（HTTP）]→[設定]の[HTTP設定：]で、[スタンドアロンモード]を選択します。

● HTTPプロキシサーバの下位にVC300bを設置する場合

設定方法

1. クライアントで利用するブラウザのHTTPプロキシサーバとしてVC300bを設定する。

2. VC300bの上位プロキシサーバとしてHTTPプロキシサーバを設定する。

 [Web(HTTP)]→[設定]の[HTTP設定：]で、[プロキシサーバを使用する]を選択し、[プロキシサーバ：]と[ポート：]に既存のプロキシサーバのIPアドレスとポート番号を入力します。

ファイル転送(FTP)の設定

InterScan VirusWallのファイル転送(FTP)検索は、お使いのシステムの設定に従って独自のFTPプロキシサーバとして設定することも、既存のFTPプロキシサーバと併用することもできます。システムの設定に応じて、InterScanコンソールの[ファイル転送(FTP)]→[設定]ページで[スタンドアロンモード]または、[FTPプロキシを使用する]のどちらかを選択します。

FTP設定：

1. InterScan VirusWallの管理コンソールで、[ファイル転送(FTP)]→[設定]を選択する。

2. [FTP設定]の[設定：]で、[スタンドアロンモード]または、[FTPプロキシを使用する：]のいずれかを選択する。

   [FTPプロキシを使用する：]を選択した場合は、FTPプロキシサーバのIPアドレスとポート番号を設定してください。

   [スタンドアロンモード]：ネットワークで唯一のFTPプロキシサーバとして動作する場合

   InterScan VirusWallのファイル転送(FTP)をシステムのFTPプロキシサーバとして使用する場合は、[スタンドアロンモード]を選択してください。クライアントからは、常にInterScanにFTP接続し、InterScanでは要求されたサイトに対する接続を確立します。クライアントでユーザ名の入力が要求された際に、ユーザ名に対象となるドメインのドメイン名をつけることを忘れないでください。たとえば、ユーザjohnがwidgets.comにFTP接続する場合の例を示します。

   − widgets.comに直接接続する場合

   ユーザ名:　　john
   パスワード:　opensesame

   − InterScan VirusWallのファイル転送(FTP)を介して接続する場合

   ユーザ名:　　john@widgets.com
   パスワード:　opensesame

   [FTPプロキシを使用する]: ネットワーク上に既存のFTPプロキシサーバがある場合

   ネットワーク上に既存のFTPプロキシサーバがある場合には、[FTPプロキシを使用する]を選択し、テキストボックスにサーバのIPアドレスとポートを入力します。InterScan VirusWallのファイル転送(FTP)では、ここで指定されたマシンに対するすべてのFTPトラフィック、およびそのマシンからのすべてのFTPトラフィックについて、ウイルス検索を実行します。

3. [FTPプロキシを使用する]を選択した場合、既存のFTPプロキシサーバのIPアドレスとポート番号を入力する。

   次に例を示します。

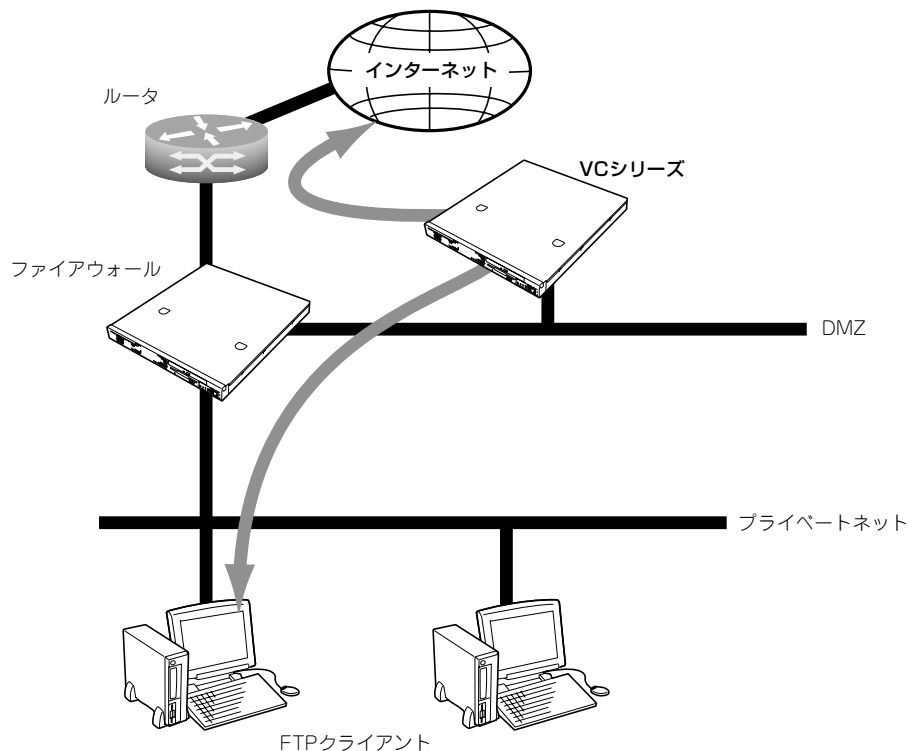
   123.12.13.123 21

重要

VC300bをFTPサーバとし、そのFTPのやりとりをInterScan VirusWall でウイルス検索させることはできません。

システムのセットアップ

InterScan VirusWallのファイル転送(FTP)導入例

● ネットワーク内にFTPプロキシサーバが存在しない場合

設定方法

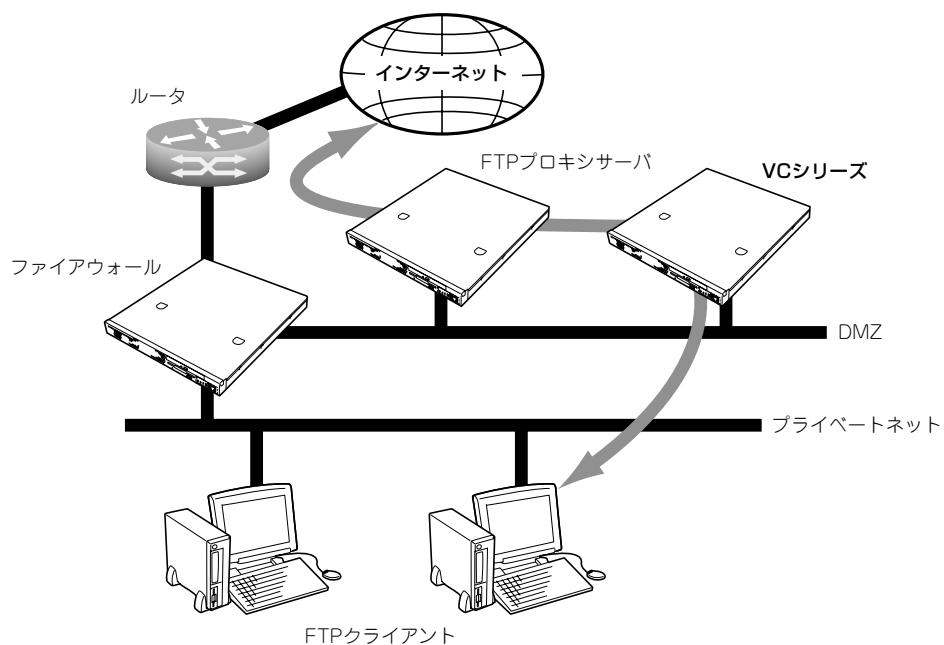
1. VC300bが直接インターネットを参照するFTPプロキシサーバとして動作するよう設定する。

   [ファイル転送(FTP)]→[設定]の[FTP設定]の[設定：]で[スタンドアロンモード]を選択する。

2. クライアントからFTPを利用する場合、VC300bに接続を行い、ユーザ名には ユーザ名@FTPサーバのホスト名 の形式で入力する。

   − ftpserver.com にユーザ名(user)、パスワード(pass)で接続する場合

   ユーザ名:　　user@ftpserver.com
   パスワード:　pass

● FTPプロキシサーバが存在する場合

設定方法

1. VC300bの上位プロキシサーバとしてFTPプロキシサーバを設定する。

[ファイル転送(FTP)]→[設定]の[FTP設定]の[設定：]で[FTPプロキシを使用する：]を選択し、既存のFTPプロキシサーバのIPアドレスとポート番号を指定する。

2. クライアントで利用するFTPクライアントのFTPプロキシサーバとしてVC300bを設定する。

ESMPRO/ServerAgentのセットアップ

ESMPRO/ServerAgentは出荷時にインストール済みですが、固有の設定がされていません。以下のオンラインドキュメントを参照し、セットアップをしてください。

添付のバックアップCD-ROM:/nec/Linux/esmpro.sa/doc

ESMPRO/ServerAgentの他にも「エクスプレス通報サービス」(5章参照)がインストール済みです。ご利用には別途契約が必要となります。詳しくはお買い求めの販売店または保守サービス会社にお問い合わせください。

シリアル接続の管理PCから設定作業をする場合は、管理者としてログインした後、設定作業を開始する前に環境変数「LANG」を「C」に変更してください。デフォルトのシェル環境の場合は以下のコマンドを実行することで変更できます。

```
#export LANG=C
```

システム情報のバックアップ

システムのセットアップが終了した後、オフライン保守ユーティリティを使って、システム情報をバックアップすることをお勧めします。
システム情報のバックアップがないと、修理後にお客様の装置固有の情報や設定を復旧(リストア)できなくなります。次の手順に従ってバックアップをしてください。

「EXPRESSBUILDER (SE) CD-ROM」からシステムを起動して操作します。「EXPRESSBUILDER (SE) CD-ROM」から起動させるためには、事前にセットアップが必要です。5章を参照して準備してください。

1. 3.5インチフロッピーディスクを用意する。
2. EXPRESSBUILDER(SE) CD-ROMを本体装置のCD-ROMドライブにセットして、再起動する。

   EXPRESSBUILDER(SE)から起動して「EXPRESSBUILDER(SE)トップメニュー」が表示されます。
3. 「ツール」ー「オフライン保守ユーティリティ」を選ぶ。
4. [システム情報の管理]から[退避]を選択する。

   以降は画面に表示されるメッセージに従って処理を進めてください。

続いて管理PCに本装置を監視・管理するアプリケーションをインストールします。次ページを参照してください。

セキュリティパッチの適用

最新のセキュリティパッチは、以下のURLよりダウンロード可能です。

http://www.express.nec.co.jp/care/index.asp

定期的に参照し、適用することをお勧めします。

管理PCのセットアップ

本装置をネットワーク上のコンピュータから管理・監視するためのアプリケーションとして、「ESMPRO/ServerManager」と「DianaScope」が用意されています。
これらのアプリケーションを管理PCにインストールすることによりシステムの管理が容易になるだけでなく、システム全体の信頼性を向上することができます。

ESMPRO/ServerManagerとDianaScopeのインストールについては5章、または「EXPRESSBUILDER (SE) CD-ROM」内のオンラインドキュメントを参照してください。

再セットアップ

再セットアップとは、システムクラッシュなどの原因でシステムが起動できなくなった場合などに、添付の「バックアップCD-ROM」を使ってハードディスクを出荷時の状態に戻してシステムを起動できるようにするものです。以下の手順で再セットアップをしてください。

保守用パーティションの作成

「保守用パーティション」とは、装置の維持・管理を行うためのユーティリティを格納するためのパーティションで、55MB程度の領域を内蔵ハードディスク上へ確保します。
システムの信頼性を向上するためにも保守用パーティションを作成することをお勧めします。保守用パーティションは、添付の「EXPRESSBUILDER (SE) CD-ROM」を使って作成します。詳しくは5章を参照してください。
保守用パーティションを作成するプロセスで保守用パーティションへ自動的にインストールされるユーティリティは、「システム診断ユーティリティ」と「オフライン保守ユーティリティ」です。

システムの再インストール

再インストールを行うと、装置内の全データが消去され、出荷時の状態に戻ります。必要なデータが装置内に残っている場合、データをバックアップしてから再インストールを実行してください。

再インストールには、本体添付の「バックアップCD-ROM」と「バックアップCD-ROM用インストールディスク」が必要です。
「バックアップCD-ROM用インストールディスク」を3.5インチフロッピーディスクドライブに、「バックアップCD-ROM」をCD-ROMドライブにそれぞれ挿入し、POWERスイッチを押して電源をONにします。

このとき、前面のシリアルポートB(COM B)に管理PCを19,200bpsの転送速度で接続すると、管理PCからログを参照することができます。

しばらくすると「バックアップCD-ROM用インストールディスク」から設定情報を読み取り、自動的にインストールを実行します。

重要

このとき、確認等は一切行われずにインストール作業が開始されるため、十分注意してください。

約30分程度でインストールが完了します。インストールが完了したら、CD-ROMが自動的にイジェクトされます。CD-ROMとフロッピーディスクの両方をドライブから取り出してください。

40分以上待っても、CD-ROMがイジェクトされず、CD-ROMへのアクセスも行われていない場合は再インストールに失敗している可能性があります。リセットして、CD-ROM/フロッピーディスクをセットし直して再度インストールを試みてください。それでもインストールできない場合は、保守サービス会社、またはお買い上げの販売店までご連絡ください。

初期導入設定用ディスクの作成

前述の「初期導入設定用ディスクの作成」を参照してください。すでに初期導入設定用ディスクを作成している場合は、パスワード情報の設定のみ再度設定し直してください。ただし、設定内容を変えたいときは、新たに初期導入用設定ディスクを作り直してください。

システムのセットアップと確認

前述の「システムのセットアップ」、「セットアップの確認」を参照してください。

ESMPRO/ServerAgentのセットアップ

「システムの再インストール」でESMPRO/ServerAgentは自動的にインストールされますが、固有の設定がされていません。以下のオンラインドキュメントを参照し、セットアップをしてください。

添付のバックアップCD-ROM:/nec/Linux/esmpro.sa/doc

ESMPRO/ServerAgentの他にも「エクスプレス通報サービス」(5章参照)も自動的にインストールされます。

シリアル接続の管理PCから設定作業をする場合は、管理者としてログインした後、設定作業を開始する前に環境変数「LANG」を「C」に変更してください。デフォルトのシェル環境の場合は以下のコマンドを実行することで変更できます。

```
#export LANG=C
```

セキュリティパッチの適用

最新のセキュリティパッチは、以下のURLよりダウンロード可能です。

http://www.express.nec.co.jp/care/index.asp

定期的に参照し、適用することをお勧めします。